

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/006073 A3

(51) International Patent Classification⁷: **G06F 1/00**

(21) International Application Number: **PCT/GB2003/002623**

(22) International Filing Date: 19 June 2003 (19.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0215334.4 2 July 2002 (02.07.2002) GB

(71) Applicant (for all designated States except US): **THE ASCENT GROUP LIMITED, [GB/GB]; Unit J2/J5, Gel-lirion Industrial Estate, Pontypridd, Rhondda Cynon Taff CF37 5SX (GB).**

(72) Inventor; and
(75) Inventor/Applicant (for US only): **JACOBS, Michael**

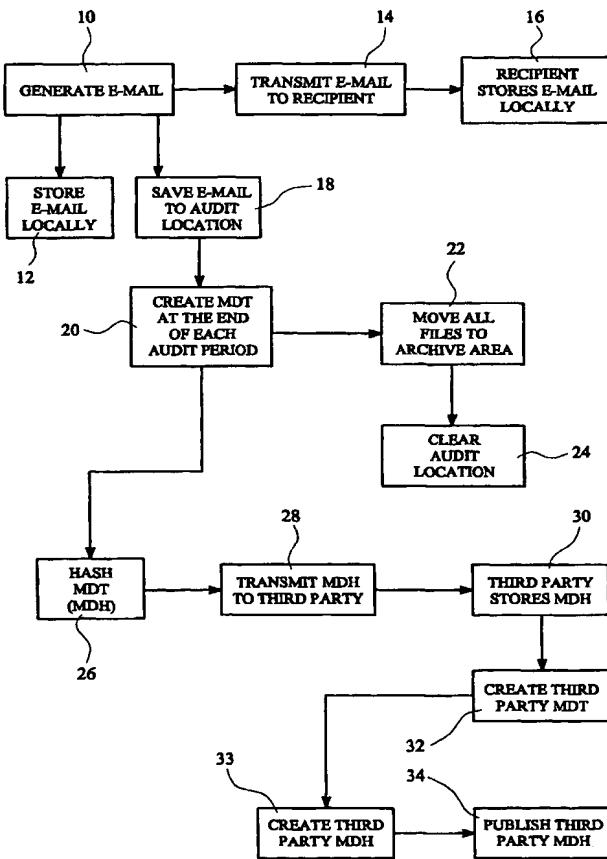
(74) Agent: **STRACHAN, Victoria, Jane; Urquhart-Dykes & Lord LLP, Alexandra House, 1 Alexandra Road, Swansea SA1 5ED (GB).**

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: STORAGE AND AUTHENTICATION OF DATA TRANSACTIONS



(57) Abstract: The various aspects of the present invention are based on four main principles: the provision, protection and validation of audit trails relating to data generated by and communicated between nodes of a network; authentication of communicating parties; enforcement of proof of receipt of data communications; and the detection of compromised user identifiers. The object of these principles being that, should a dispute arise over the substance of an authenticated e-mail or other data item, it would be possible to prove, with mathematical precision, the following features of the communication: the content of the message sent; the e-mail location to which the message was addressed; the fact that the message was despatched; the time and date of despatch; the fact that the message was received; the time and date it was received; and the fact that the content of the message had not been changed since it was sent. It is also intended to make it possible to prove the identity of the sender and the identity of the recipient.

WO 2004/006073 A3



SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:

24 June 2004

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 03/02623A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 056 010 A (HEWLETT PACKARD CO) 29 November 2000 (2000-11-29) abstract; figure 5 paragraphs [0009] - [0020]	1-9
A	SCHNEIER B: "ONE-WAY HASH FUNCTIONS" DR. DOBB'S JOURNAL, M&T PUBL., REDWOOD CITY, CA, US, vol. 16, no. 9, 1 September 1991 (1991-09-01), pages 148-151, XP002044823 ISSN: 1044-789X page 150, column 2	1-9

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

19 February 2004

29.04.2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Kerschbaumer, J

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 03/02623

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIER B: "DIGITAL SIGNATURES" BYTE, MCGRAW-HILL INC. ST PETERBOROUGH, US, vol. 18, no. 12, 1 November 1993 (1993-11-01), pages 309-312, XP000408886 ISSN: 0360-5280 page 311, column 2, paragraph 3 -----	1-9
A	WO 02/48843 A (SILANIS TECHNOLOGY INC) 20 June 2002 (2002-06-20) abstract; figure 1 page 2, line 25 - page 3, line 29 -----	1-9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB 03/02623

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.: because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-9

Remark on Protest

The additional search fees were accompanied by the applicant's protest.

No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9

Non repudiation of data items by transmitting hashes of the data items to a remote location

2. claims: 10-19

Tracability of data transmissions between first and second users by encrypting and acknowledgement via different identifiers

3. claims: 20-23

Authentication of data items communicated from a first user to a second user.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 03/02623

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
EP 1056010	A	29-11-2000	EP	1056010 A1		29-11-2000
			EP	1181642 A1		27-02-2002
			WO	0073904 A1		07-12-2000
<hr/>						
WO 0248843	A	20-06-2002	AU	1578202 A		24-06-2002
			WO	0248843 A2		20-06-2002
			CA	2428665 A1		20-06-2002
			EP	1393144 A2		03-03-2004
			US	2002091651 A1		11-07-2002
<hr/>						